

REMARKS

Reconsideration of the application in view of the above amendments and the following remarks is respectfully requested. Claims 1 and 17 have been amended. Claims 3 and 19 have been reinstated. Claims 1, 3-17, and 19-32 are currently pending in the application.

In the Final Office Action mailed on March 6, 2006, the Examiner stated that claims 3 and 19 would be allowable if rewritten in independent form to include all of the limitations of the base claims and any intervening claims. Relying upon this statement, Applicant amended independent claims 1 and 17 to incorporate the limitations of claims 3 and 19, respectively, and canceled claims 3 and 19. However, in the subsequent Office Action mailed on October 4, 2006, the Examiner rejected claims 1 and 17. Thus, it appears that the Examiner's mind has changed. In response to this turn of events, Applicant has amended claims 1 and 17 to put them back into the state they were in before the most recent amendment. Applicant has also reinstated claims 3 and 19.

Rejections Under 35 U.S.C. §103

In the Office Action, the Examiner rejected claims 1, 4-17, and 20-32 under 35 U.S.C. §103(a) as being unpatentable over Schnurer et al. (U.S. Patent No. 5,842,002, hereinafter, Schnurer) in view of Nachenberg (U.S. Patent No. 6,357,008) and further in view of Basu et al. (U.S. Patent No. 6,836,888, hereinafter, Basu). This rejection is respectfully traversed.

Claim 1

Claim 1 recites:

A computer-implemented method for executing an untrusted program, comprising:

establishing a limited environment within a general environment, wherein said limited environment comprises one or more mock resources, wherein said general environment comprises one or more real resources, wherein said limited environment and said general environment are both provided by the same operating system, and wherein programs executing within said limited environment cannot access the one or more real resources in said general environment;

executing at least a portion of an untrusted program within said limited environment; and

examining said limited environment after execution of at least said portion of said untrusted program to check for undesirable behavior exhibited by said untrusted program. (Emphasis added)

Claim 1 makes it clear that the untrusted program is actually executed within the limited environment. As is well known in the computer arts, the execution of a program involves the execution of the instructions in the program. This execution is typically carried out by having a set of native hardware (e.g. a processor) execute the machine language instructions that make up the compiled version of the program. Execution is quite different from emulation. With emulation, the instructions of a program are not actually executed by a processor. Rather, the behavior of the program is imitated. As stated in the discussion of "emulator" in Wikipedia:

Emulation refers to the ability of a program or device to imitate another program or device.

Emulation attempts to model to various degrees the state of the device being emulated.

Both the OS and the software will be interpreted by the emulator, rather than being run by native hardware. (Emphasis added)

From these excerpts, it is clear that when a program is emulated, the instructions of that program are not executed. Rather, the behavior of the program is just modeled and imitated.

None of the applied references disclose or suggest executing an untrusted program in a limited environment. With regard to Schnurer, there is ample support for the position that a potential virus is not executed but rather is emulated in a limited environment. For example, Schnurer refers to the component that intercepts the potential virus code before it enters the protected computer system as the "emulation box" (See Fig. 1) or the "emulation means" (See Col. 7, line 3-5). Schnurer also specifically states that when the trapping device is started, emulation software is read and executed (See Col. 7, lines 19-20). Furthermore, Schnurer states in Col. 6, lines 2-7:

This scheme is based on the assumptions that almost all viruses are executable in nature, no user would try to purposely communicate a destructive virus to another and that it is possible to identify executable instructions in an environment where the instruction cannot possibly operate. (Emphasis added)

The underlined portion of the above excerpt basically says that, in Schnurer, the potentially malignant virus code is identified in an environment in which the instructions of the virus cannot possibly operate (i.e. cannot possibly execute). From these excerpts, and from an overall reading of Schnurer, it is clear that the potential virus code is not executed within the trapping device of Schnurer. Rather, the trapping device emulates the behavior of the virus code. Because Schnurer discloses emulation rather than actual execution, Applicant submits that the "executing at least a portion of an untrusted program within said limited environment" limitation of claim 1 is not disclosed or suggested by Schnurer.

Nachenberg also fails to disclose or suggest this aspect of claim 1. Like Schnurer, Nachenberg also discloses emulating the behavior of a set of potential virus code rather than actually executing the virus code. For example, in Col. 7, lines 3-5, Nachenberg states:

A purpose of the decryption phase 252 is to emulate a sufficient number of instructions to allow an encrypted virus to decrypt its viral body. (Emphasis added)

Furthermore, in Col. 7, lines 9-11, Nachenberg states:

A purpose of the exploration phase 254 is to emulate at least once all sections of code within a region likely to contain any virus present.... (Emphasis added)

From these excerpts, and from an overall reading of Nachenberg, it is clear that the potential virus code is not executed within the virtual environment of Nachenberg. Rather, the CPU emulator 158 (See Fig. 158) emulates the behavior of the virus code in the virtual environment. Because Nachenberg discloses emulation rather than actual execution, Applicant submits that the "executing at least a portion of an untrusted program within said limited environment" limitation of claim 1 is not disclosed or suggested by Schnurer.

Basu also fails to disclose or suggest this aspect of claim 1. There is nothing in Basu that discloses or even discusses executing an untrusted program in a limited environment.

As the above discussion shows, none of the applied references disclose or suggest the "executing at least a portion of an untrusted program within said limited environment" limitation of claim 1. Thus, even if these references were combined (assuming for the sake of argument that it would have been obvious to combine the references), they would still not give rise to the method set forth in claim 1. For at least

this reason, Applicant submits that claim 1 is patentable over Schnurer, Nachenberg, and Basu, taken individually or in combination.

Applicant also submits that claims 3-16, which depend from claim 1, and which recite further advantageous aspects of the invention, are likewise patentable over Schnurer, Nachenberg, and Basu for at least the same reasons as those given above in connection with claim 1.

Claim 17

Claim 17 is a computer readable medium claim which is analogous to the method of claim 1. Thus, Applicant submits that claim 17 is patentable over Schnurer, Nachenberg, and Basu for at least the same reasons as those given above in connection with claim 1.

Applicant also submits that claims 19-32, which depend from claim 17, and which recite further advantageous aspects of the invention, are likewise patentable over Schnurer, Nachenberg, and Basu for at least the same reasons as those given above in connection with claim 17.

CONCLUSION

For the reasons given above, Applicant submits that the pending claims are patentable over the art of record, including the art cited but not applied. Accordingly, allowance of all pending claims is respectfully solicited.

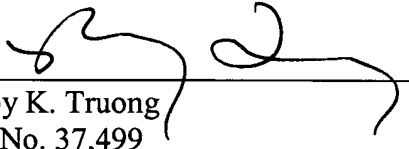
The Examiner is invited to telephone the undersigned at (408) 414-1080 to discuss any issues that may advance prosecution.

No fee is believed to be due in connection with this response. In the event that a fee is due, the Commissioner is authorized to charge any fee that may be due to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: 11/28, 2006


Bobby K. Truong
Reg. No. 37,499

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: **Mail Stop Amendment** Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

On 11/28, 2006

By 